Amendments to the Claims

This listing of claims replaces prior versions:

Claim 1 (currently amended): A data distribution system for distributing at least a license key for decrypting encrypted content data between said license key and said encrypted content data to each of terminals of a plurality of users from a content data supply device, comprising:

a first interface unit ~~(350)~~ for externally transmitting data;

a first session key generating unit ~~(314)~~ for producing a first symmetric key to be updated in response to every transmission of said license key;

a session key encryption processing unit ~~(316)~~ for encrypting said first symmetric key with a first public encryption key, and applying the encrypted first symmetric key to said first interface unit;

a session key decrypting unit ~~(318)~~ for decrypting a second symmetric key and a second public encryption key returned after being encrypted with said first symmetric key based on said first symmetric key to extract said second symmetric key and said second public encryption key;

a first license data encryption processing unit ~~(320)~~ for encrypting said license key with said second public encryption key extracted by said session key decrypting unit; and

a second license data encryption processing unit ~~(822)~~ for further encrypting the output of said first license data encryption processing unit with said second symmetric key extracted by said session key decrypting unit, and supplying the encrypted output to said first interface unit, wherein

each of said terminals includes:

a second interface unit for externally transmitting the data, and

a data storing unit ~~(140)~~ for receiving and storing at least said license key from said content data supply device;

said first public encryption key is predetermined for said data storing unit; and

said data storing unit includes:

a first key holding unit ~~(1402)~~ for holding a first private decryption key for decrypting the data encrypted with said first public encryption key,

a first decryption processing unit ~~(1404)~~ for receiving and decrypting said first symmetric key encrypted with said first public encryption key,

a second key holding unit ~~(1405)~~ for holding said second public encryption key,

a second session key generating unit ~~(1432)~~ for producing said second symmetric key,

a first encryption processing unit ~~(1406)~~ for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said second interface unit,

a second decryption processing unit ~~(1410)~~ for receiving said license key encrypted with said second symmetric key, further encrypted with said second public encryption key and applied from said second license data encryption processing unit, and decrypting the received license key based on said second symmetric key,

a third key holding unit ~~(1415)~~ for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit,

a third decryption processing unit ~~(1416)~~ for receiving said license key encrypted with said second public encryption key, and decrypting the received license key with said second private decryption key for extraction, and

a memory unit ~~(1412)~~ for storing said encrypted content data and said license key.

Claim 2 (currently amended): The data distribution system according to claim 1, wherein each of said terminals further includes a content reproducing unit;

said content reproducing unit includes:

a fourth key holding unit ~~(1520)~~ for holding a third private decryption key used for decrypting the data encrypted with said third public encryption key,

a fourth decryption processing unit ~~(1522)~~ for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit,

a third session key generating unit ~~(1502)~~ for producing a third symmetric key,

a second encryption processing unit ~~(1504)~~ for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key,

a fifth decryption processing unit ~~(1506)~~ for decrypting and extracting said license key encrypted based on said third symmetric key in said data storing unit, and

a data reproducing unit ~~(1508)~~ for receiving said encrypted content data recorded in said memory unit from said data storing unit, and decrypting said encrypted content data with said extracted license key for reproduction;

said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key; and

said data storing unit sends instructions to receive by said content reproducing unit said third symmetric key encrypted with said second symmetric key, to encrypt by said first encryption processing unit said license key stored in said memory unit with said third symmetric key decrypted and extracted based on said second symmetric key by said second decryption processing unit ~~(1410)~~, and to output the encrypted license key to said content reproducing unit.

Claim 3 (currently amended): The data distribution system according to claim 1, wherein said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key of a different data storing unit in a transfer processing for transferring at least said license key to said different data storing unit, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said fourth encryption processing unit encrypts said license key stored in said memory unit with the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 4 (previously presented): The data distribution system according to claim 3, wherein

transfer accepting processing of said data storing unit for receiving said license key transferred from said different data storing unit in accordance with transfer processing of said different data storing unit is performed such that:

said first decryption processing unit decrypts and extracts said second symmetric key encrypted with said first public encryption key and generated by said different data storing unit in said transfer acceptance processing,

said second session key generating unit generates said fourth symmetric key in accordance with said transfer acceptance processing,

said first encryption processing unit encrypts said second public encryption key and said fourth symmetric key with said second symmetric key for output the encrypted keys in accordance with said transfer acceptance processing, and

said second decryption processing unit decrypts with said fourth symmetric key the license key encrypted with said second public encryption key of said different data storing unit, and further encrypted with said fourth symmetric key.

Claim 5 (previously presented): The data distribution system according to claim 1, wherein

said memory unit receives the output of said second decryption processing unit, and stores said license key encrypted with said second public encryption key, and

said third decryption processing unit decrypts said license key encrypted with said second public encryption key stored in said memory unit with said second private decryption key.

Claim 6 (previously presented): The data distribution system according to claim 1, wherein

said third decryption processing unit receives the output of said second decryption processing unit, and decrypts said license key encrypted with said second public encryption key with said second private decryption key, and

said memory unit receives the output of said third decryption processing unit, and stores said license key.

Claim 7 (currently amended): A data supply device for supplying at least a license key for decrypting encrypted content data between said license key and said encrypted content data to each of a plurality of user terminals provided with a data storing unit capable of storing at least said license key, comprising:

an interface unit ~~(350)~~ for externally transmitting data;

a session key generating unit ~~(314)~~ for producing a first symmetric key to be updated in response to every transmission of said license key;

a session key encryption processing unit ~~(316)~~ for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said data storing unit of said user terminal, and applying the encrypted first symmetric key to said interface unit;

a session key decrypting unit ~~(318)~~ for decrypting and extracting a second symmetric key and a second public encryption key returned after being encrypted with said first symmetric key;

a first license data encryption processing unit ~~(320)~~ for encrypting said license key for decrypting said encrypted content data with said second public encryption key decrypted by said session key decrypting unit; and

a second license encryption processing unit ~~(322)~~ for further encrypting the output of said first license data encryption processing unit with said second symmetric key, and applying the encrypted output to said interface unit for supply to each of said terminals.

Claim 8 (previously presented): The data supply device according to claim 7, wherein

said first public encryption key is applied from said terminal via said interface unit, and

said session key encryption processing unit encrypts said first symmetric key with said applied first public encryption key.

Claim 9 (currently amended): The data supply device according to claim 7, wherein

said data supply device further includes:

an authentication key holding unit for holding an authentication key,

an authentication decryption processing unit ~~(326)~~ for decrypting and extracting authentication data being decodable with said authentication key, obtained from said terminal via said interface unit and predetermined for said data storing unit of said terminal, and

a control unit ~~(312)~~ for performing authentication processing based on said authentication data extracted by said authentication decryption processing unit, and determining whether at

least the license key is to be supplied to the terminal providing said obtained authentication data or not.

Claim 10 (previously presented): The data supply device according to claim 9, wherein

said first public encryption key is obtained from each of said terminals via said interface unit after being encrypted together with said authentication data into a form decodable with said authentication key, and

said authentication data decryption processing unit decrypts with said authentication key said authentication data and said first public encryption key obtained via said interface unit and encrypted into a form decodable with said authentication key, extracts said authentication data and said first public encryption key, and outputs said extracted authentication data and said extracted first public encryption key to said control unit and said session key encryption processing unit, respectively.

Claim 11 (previously presented): The data supply device according to claim 7, wherein

said data supply device includes:

an encryption key holding unit for holding a terminal common encryption key for performing encryption allowing decryption in each of said terminals, and

a third license encryption processing unit for encrypting said license key with said terminal common encryption key held in said encryption key holding unit, and outputting the encrypted license key to said first license encryption processing unit.

Claim 12 (currently amended): A data supply device for supplying at least a license key for decrypting encrypted content data between said license key and said encrypted content data to a plurality of recording devices, comprising:

an interface unit ~~(350)~~ for transmitting data to and from said recording device;

a connecting unit ~~(2010, 2030)~~ for connecting said interface unit and said recording device for supply of the data;

a first session key generating unit ~~(314)~~ for producing a first symmetric key to be updated in response to every supply of said license key;

a session key encryption processing unit ~~(316)~~ for encrypting said first symmetric key with a first public encryption key predetermined corresponding to said recording device, and applying the encrypted first symmetric key to said interface unit;

a session key decrypting unit ~~(318)~~ for decrypting and extracting a second symmetric key and a second public encryption key applied from the recording device connected to said connecting unit after being encrypted with said first symmetric key;

a first license data encryption processing unit ~~(320)~~ for encrypting said license key for decrypting said encrypted content data with said second public encryption key decrypted by said session key decrypting unit; and

a second license encryption processing unit ~~(322)~~ for further encrypting the output of said first license data encryption processing unit with said second symmetric key, and applying the encrypted output to said interface unit for supply to said recording device connected to the connecting unit.

Claim 13 (previously presented): The data supply device according to claim 12, wherein each of said recording devices is a memory card, and

said recording device can be directly connected to said memory card.

Claim 14 (previously presented): The data supply device according to claim 12, wherein

said first public encryption key is applied from each of said recording devices via said interface unit, and

said session key encryption processing unit encrypts said first symmetric key with said applied first public encryption key.

Claim 15 (currently amended): The data supply device according to claim 12, further comprising:

an authentication decryption processing unit ~~(326)~~ for decrypting and extracting authentication data being decodable with an authentication key, and obtained from said recording device via said interface unit, and

a control unit ~~(312)~~ for performing authentication processing based on said authentication data extracted by said authentication decryption processing unit, and determining whether at least the license key is to be output to said recording device or not.

Claim 16 (previously presented): The data supply device according to claim 15, wherein

said first public encryption key is obtained from said recording devices via said interface unit after being encrypted together with said authentication data into a form decodable with said authentication key, and

said authentication data decryption processing unit decrypts with said authentication key said authentication data and said first public encryption key obtained via said interface unit and encrypted into a form decodable with said authentication key, extracts said authentication data and said first public encryption key, and outputs said extracted authentication data and said extracted first public encryption key to said control unit and said session key encryption processing unit, respectively.

Claim 17 (currently amended): The data supply device according to claim [[10]] 12, wherein

said data supply device includes:

an encryption key holding unit ~~(330)~~ attached to said recording device for obtaining said license key and said encrypted content data stored in said recording device, and holding a terminal common encryption key for performing encryption allowing decryption by a plurality of terminals decrypting said encrypted content data to obtain the content data, and

a third license encryption processing unit ~~(332)~~ for encrypting said license key based on said terminal common encryption key held in said encryption key holding unit, and outputting the encrypted license key to said first license encryption processing unit.

Claim 18 (previously presented): The data supply device according to claim 12, wherein

said recording device includes means for changing the number of terminals connected to said interface unit for externally receiving the data, and performing switching between a serial mode for performing data communication on a bit-by-bit basis and a parallel mode for performing data communication by multiple bits at a time;

said data supply device supplies said encrypted content data together with said license key to said recording device via said interface unit; and

said interface unit instructs the parallel mode to said recording device when at least said encrypted content data is to be input to said recording device.

Claim 19 (currently amended): A terminal device for receiving at least a license key for decrypting encrypted content data between said license key and said encrypted content data distributed from a data supply device, comprising:

a first interface unit for externally transmitting data; and

a data storing unit ~~(140)~~ for receiving and storing said license key, wherein

said data storing unit includes:

a first key holding unit ~~(1402)~~ for holding a first private decryption key for decrypting the data encrypted with a first public encryption key,

a first decryption processing unit ~~(1404)~~ for receiving and decrypting a first symmetric key encrypted with said first public encryption key and externally input,

a second key holding unit ~~(1405)~~ for holding a second public encryption key unique to said data storing unit,

a second session key generating unit ~~(1432)~~ for producing a second symmetric key,

a first encryption processing unit ~~(1406)~~ for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said first interface unit,

a second decryption processing unit ~~(1410)~~ for receiving the license key encrypted with said second public encryption key and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key,

a third key holding unit ~~(1415)~~ for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit,

a memory unit ~~(1412)~~ for receiving the output of said second decryption processing unit, and storing said license key encrypted with said second public encryption key, and

a third decryption processing unit ~~(1416)~~ for receiving the license key encrypted with said second public encryption key stored in said memory unit, and decrypting the received license key with said second private decryption key.

Claim 20 (previously presented): The terminal device according to claim 19, wherein said data storing unit is a recording device releasably attached to said terminal device.

Claim 21 (currently amended): The terminal device according to claim 19, wherein said data storing unit further includes a fourth key holding unit ~~(1401)~~ holding said first public encryption key and being capable of externally outputting said first public encryption key.

Claim 22 (currently amended): The terminal device according to claim 19, wherein said data storing unit further includes a first data holding unit ~~(1442)~~ for encrypting and holding said first public encryption key and first authentication data unique to said data storing

unit and determined uniquely to said first public encryption key in a form allowing decryption with a predetermined authentication key.

Claim 23 (currently amended): The terminal device according to claim 19, wherein

said terminal device further includes a content reproducing unit;

said content reproducing unit includes:

a fifth key holding unit ~~(1520)~~ for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key unique to said content reproducing unit,

a fourth decryption processing unit ~~(1522)~~ for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit,

a third session key generating unit ~~(1502)~~ for producing a third symmetric key,

a second encryption processing unit ~~(1504)~~ for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key,

a fifth decryption processing unit ~~(1506)~~ for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit, and

a data reproducing unit ~~(1508)~~ for decrypting the encrypted content data recorded in said recording unit with said extracted license key to reproduce the content data;

said data storing unit further includes a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key;

said second decryption processing unit ~~(1410)~~ further receives said third symmetric key encrypted with said second symmetric key in said content reproducing unit, and decrypts said encrypted third symmetric key based on said second symmetric key to extract said third symmetric key;

said third decryption processing unit decrypts said license key encrypted with said second public encryption key stored in said memory unit based on said second private decryption key, and extracts said license key; and

said first encryption processing unit further encrypts said license key extracted by said third decryption processing unit based on said third symmetric key extracted by said second decryption processing unit, and applies the encrypted license key to said content reproducing unit.

Claim 24 (currently amended): The terminal device according to claim 23, wherein

said content reproducing unit further includes a sixth key holding unit ~~(1524)~~ for holding said third public encryption key, and being capable of externally outputting said third public encryption key.

Claim 25 (currently amended): The terminal device according to claim 23, wherein

said content reproducing unit includes a second data holding unit ~~(1525)~~ for encrypting and holding said third public encryption key and second authentication data being unique to said data storing unit and determined uniquely with respect to the third public encryption key such that said third public encryption key and said second authentication data can be decrypted with a predetermined authentication key;

said data storing unit further includes:

an authentication key holding unit for holding said authentication key,

an authentication data decryption processing unit for decrypting said second authentication data applied from said data storing unit based on said authentication key to extract said third public encryption key and said first authentication data, and

a control unit ~~(1420)~~ for performing authentication based on said second authentication data, and determining whether at least the license key is to be output to said content reproducing unit or not; and

said authentication data decryption processing unit applies said extracted third public encryption key and said extracted second authentication data to said third encryption processing unit and said control unit, respectively.

Claim 26 (previously presented): The terminal device according to claim 23, wherein

said license key is stored in the memory unit after being encrypted into a form allowing decryption with a terminal common decryption key common to said plurality of terminals;

said content reproducing unit further includes:

a decryption key holding unit for holding said terminal common decryption key, and

a sixth decryption processing unit for decrypting the output of said fifth decryption processing unit based on said terminal common decryption key to extract said license key.

Claim 27 (currently amended): The terminal device according to claim 19, wherein

said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key of a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key;

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 28 (currently amended): The terminal device according to claim 21, wherein said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key applied from a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key;

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 29 (currently amended): The terminal device according to claim 20, wherein said data storing unit further includes:

an authentication key holding unit for holding said authentication key,

an authentication data decryption processing unit for decrypting said first authentication data applied from a different data storing unit based on said authentication key to extract said first public encryption key and said first authentication data in accordance with transfer processing for transferring at least said license key to said different data storing unit,

a control unit ~~(1420)~~ for performing authentication based on said first authentication data and in accordance with said transfer processing, and determining whether at least the license key is to be output to said different data storing unit or not,

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key output from said different data storing unit in accordance with said transfer processing, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key;

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 30 (currently amended): A terminal device for receiving at least a license key for decrypting encrypted content data between said license key and said encrypted content data distributed from a data supply device, comprising:

a first interface unit for externally transmitting data; and

a data storing unit ~~(140)~~ for receiving and storing said license key, wherein

said data storing unit includes:

a first key holding unit ~~(1402)~~ for holding a first private decryption key for decrypting the data encrypted with a first public encryption key,

a first decryption processing unit ~~(1404)~~ for receiving and decrypting a first symmetric key encrypted with said first public encryption key and externally input,

a second key holding unit ~~(1405)~~ for holding a second public encryption key unique to said data storing unit,

a second session key generating unit ~~(1432)~~ for producing a second symmetric key,

a first encryption processing unit ~~(1406)~~ for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said first interface unit,

a second decryption processing unit ~~(1410)~~ for receiving the license key encrypted with said second public encryption key and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key,

a third key holding unit ~~(1415)~~ for holding a second private decryption key used for decrypting the data encrypted with said second public encryption key and being unique to said data storing unit,

a third decryption processing unit ~~(1416)~~ for receiving said license key encrypted with said second public encryption key, and decrypting the received license key with said second private decryption key, and

a memory unit ~~(1412)~~ for receiving the output of said third decryption processing unit, and storing said license key.

Claim 31 (previously presented): The terminal device according to claim 30, wherein said data storing unit is a recording device releasably attached to said terminal device.

Claim 32 (currently amended): The terminal device according to claim 30, wherein said data storing unit further includes a fourth key holding unit ~~(1401)~~ holding said first public encryption key and being capable of externally outputting said first public encryption key.

Claim 33 (currently amended): The terminal device according to claim 30, wherein said data storing unit further includes a first data holding unit ~~(1442)~~ for encrypting and holding said first public encryption key and first authentication data unique to said data storing

unit and determined uniquely to said first public encryption key in a form allowing decryption with a predetermined authentication key.

Claim 34 (currently amended): The terminal device according to claim 21, wherein

said terminal device further includes a content reproducing unit;

said content reproducing unit includes:

a fifth key holding unit ~~(1520)~~ for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key predetermined for said content reproducing unit,

a fourth decryption processing unit ~~(1522)~~ for decrypting and extracting said second symmetric key encrypted with said third public encryption key in said data storing unit,

a third session key generating unit ~~(1502)~~ for producing a third symmetric key,

a second encryption processing unit ~~(1504)~~ for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key,

a fifth decryption processing unit ~~(1506)~~ for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit, and

a data reproducing unit ~~(1508)~~ for decrypting the encrypted content data recorded in said recording unit with said extracted license key to reproduce the content data;

said data storing unit further includes a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key produced by said second session key generating unit based on said third public encryption key;

said second decryption processing unit ~~(1410)~~ further receives said third symmetric key encrypted with said second symmetric key in said content reproducing unit, and decrypts said encrypted third symmetric key based on said second symmetric key to extract said third symmetric key; and

said first encryption processing unit further encrypts said license key stored in said memory unit based on said third symmetric key extracted by said second decryption processing unit, and applies the encrypted license key to said content reproducing unit.

Claim 35 (currently amended): The terminal device according to claim 34, wherein

said content reproducing unit further includes a sixth key holding unit ~~(1524)~~ for holding said third public encryption key, and being capable of externally outputting said third public encryption key.

Claim 36 (currently amended): The terminal device according to claim 34, wherein

said content reproducing unit includes a second data holding unit ~~(1525)~~ for encrypting and holding said third public encryption key and second authentication data being unique to said data storing unit and determined uniquely with respect to the third public encryption key such that said third public encryption key and said second authentication data can be decrypted with a predetermined authentication key;

said data storing unit further includes:

an authentication key holding unit for holding said authentication key,

an authentication data decryption processing unit for decrypting said second authentication data applied from said data storing unit based on said authentication key to extract said third public encryption key and said first authentication data, and

a control unit ~~(1420)~~ for performing authentication based on said second authentication data, and determining whether at least the license key is to be output to said content reproducing unit or not; and

said authentication data decryption processing unit applies said extracted third public encryption key and said extracted second authentication data to said third encryption processing unit and said control unit, respectively.

Claim 37 (previously presented): The terminal device according to claim 34, wherein

said license key is stored in the memory unit after being encrypted into a form allowing decryption with a terminal common decryption key common to said plurality of terminals;

said content reproducing unit further includes:

a decryption key holding unit for holding said terminal common decryption key, and

a sixth decryption processing unit for decrypting the output of said fifth decryption processing unit based on said terminal common decryption key to extract said license key.

Claim 38 (currently amended): The terminal device according to claim 30, wherein

said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key of a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said fourth encryption processing unit encrypts said extracted license key stored in said memory unit based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 39 (currently amended): The terminal device according to claim 38, wherein

said data storing unit further includes a fourth key holding unit ~~(1401)~~ holding said first public encryption key and being capable of externally outputting said first public encryption key, and

said third encryption processing unit performs encryption based on said first public encryption key applied from said different data storing unit in accordance with said transfer processing.

Claim 40 (currently amended): The terminal device according to claim 32, wherein

said data storing unit further includes:

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key output from a different data storing unit in accordance with a transfer processing for transferring at least said license key to said different data storing unit, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key;

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 41 (currently amended): The terminal device according to claim 33, wherein

said data storing unit further includes:

an authentication key holding unit for holding said authentication key,

an authentication data decryption processing unit for decrypting said first authentication data applied from a different data storing unit based on said authentication key to extract said first public encryption key and said first authentication data in accordance with transfer processing for transferring at least said license key to said different data storing unit,

a control unit ~~(1420)~~ for performing authentication based on said first authentication data and in accordance with said transfer processing, and determining whether at least the license key is to be output to said different data storing unit or not,

a third encryption processing unit ~~(1430)~~ for encrypting said second symmetric key with said first public encryption key output from said different data storing unit in accordance with said transfer processing, and

a fourth encryption processing unit ~~(1414)~~ for performing the encrypting processing with the second public encryption key of said different data storing unit;

said second session key generating unit generates said second symmetric key in accordance with said transfer processing;

said second decryption processing unit decrypts and extracts a fourth symmetric key applied from said different data storing unit after being encrypted with said second symmetric key and the second public encryption key of said different data storing unit in accordance with said transfer processing;

said third decryption processing unit decrypts the data encrypted with said second public encryption key stored in said memory unit based on said second private decryption key in accordance with said transfer processing to extract said license key;

said fourth encryption processing unit encrypts said extracted license key based on the second public encryption key of said different data storing unit in accordance with said transfer processing; and

said first encryption processing unit encrypts the output of said fourth encryption processing unit with said extracted fourth symmetric key, and outputs the encrypted output to said different data storing unit in accordance with said transfer processing.

Claim 42 (currently amended): A terminal device for receiving at least a license key for decrypting encrypted content data between said license key and said encrypted content data distributed from a data supply device, comprising:

a first interface unit for transmitting data to and from said data supply device;

a content reproducing unit; and

a second interface unit for connection to a data storing unit releasably attached to said terminal device, wherein

said content reproducing unit includes:

a fourth key holding unit ~~(1520)~~ for holding a third private decryption key used for decrypting the data encrypted with a third public encryption key,

a fourth decryption processing unit ~~(1522)~~ for decrypting and extracting [[said]] a second symmetric key encrypted with said third public encryption key in said data storing unit,

a third session key generating unit ~~(1502)~~ for producing a third symmetric key,

a second encryption processing unit ~~(1504)~~ for encrypting said third symmetric key based on said second symmetric key decrypted and extracted by said fourth decryption processing unit, and outputting the encrypted third symmetric key,

a fifth decryption processing unit ~~(1506)~~ for decrypting and extracting the license key encrypted with said third symmetric key in said data storing unit, and

a data reproducing unit ~~(1508)~~ for decrypting the encrypted content data recorded in said recording unit with the extracted license key to reproduce the content data.

Claim 43 (currently amended): The terminal device according to claim 42, further comprising:

a data holding unit ~~(1525)~~ for holding second authentication data and said third public encryption key in a form allowing decryption with an authentication key for external output.

Claim 44 (currently amended): A recording device for storing an encrypted content data and a license key for decrypting said encrypted content data, comprising:

an interface unit for externally transmitting data;

a memory unit ~~(1412)~~ for recording the data; and

a parallel data bus ~~(BS3)~~ having a width of m bits (m is a natural number larger than 1 ($m > 1$)), and transmitting the data between said interface unit and said recording unit, wherein

said interface unit includes:

a plurality of terminals ~~(1462.0 – 1462.3)~~,

selecting means for selecting a predetermined terminal(s) of one or n in number (n is a natural satisfying ($1 < n \leq m$)) as a terminal(s) for externally receiving data in accordance with a switching instruction for a bit width of the externally applied input data,

first converting means for operating in accordance with said switching instruction to convert serial data externally applied via said selected one terminal or parallel data of an n-bit width externally applied via said n terminals into parallel data of an m-bit width, and supply the converted parallel data to said parallel data bus, and

second converting means for converting the parallel data of the m-bit width applied from said parallel data bus into serial data, and externally outputting the converted serial data via predetermined one terminal among said plurality of terminals;

a first key holding unit ~~(1402)~~ for holding a first private decryption key for decrypting data encrypted with a first public encryption key;

a first decryption processing unit ~~(1404)~~ for receiving a first symmetric key encrypted with said first public encryption key, and decrypting the received first symmetric key based on said first private decryption key;

a second key holding unit ~~(1405)~~ for holding a second public encryption key;

a session key generating unit ~~(1432)~~ for producing a second symmetric key;

a first encryption processing unit ~~(1406)~~ for encrypting said second public encryption key and said second symmetric key based on said first symmetric key, and outputting the encrypted keys to said interface unit via said parallel data bus;

a second encryption processing unit ~~(1410)~~ for receiving a license key encrypted with said second public encryption key, and further encrypted with said second symmetric key, and decrypting the received license key based on said second symmetric key;

a third key holding unit ~~(1415)~~ for holding a second private decryption key set uniquely to said recording device for decrypting the data encrypted with said second public encryption key; and

a third decryption processing unit ~~(1416)~~ for receiving the license key encrypted with said second public encryption key, and decrypting the received license key based on said second private decryption key to extract said license key, wherein

said recording unit stores said encrypted content data and said license key.

Claim 45 (currently amended): The recording device according to claim 44, further comprising:

an authentication data holding unit ~~(1442)~~ for holding an authentication data prepared by encrypting said first public encryption key and a certificate data corresponding to said first public encryption key in a form allowing external decryption with an authentication key for external output.

Claim 46 (canceled)